SIFMA
Securities Industry and
Financial Markets Association

January 19, 2007

Via Electronic Mail

Federal Identity Theft Task Force
c/o Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Federal Identity Theft Task Force

Ladies and Gentlemen:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the Federal Identity Theft Task Force's (the "Task Force") request for public comment on issues relating to combating identity theft. The Task Force's notice indicates that the information provided by commenters will be considered by the Task Force in connection with its formulation of a final strategic plan to address identity theft.

The securities industry has long recognized the importance of protecting sensitive customer information from misuse. Member firms work diligently to effectively implement security policies and procedures to prevent identity theft. SIFMA supports the goal of further improving the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection and prosecution. Accordingly, SIFMA is pleased to provide the views of the securities industry on issues raised by the Task Force.

SOCIAL SECURITY NUMBERS

The Task Force is considering recommending certain measures to further enhance the protection of Social Security Numbers ("SSNs") to keep them out of the hands of identity thieves. Such measures include studying how SSNs are used in the private sector

[1] The Securities Industry and Financial Markets Association brings together the shared interests of more than 650 securities firms, banks and asset managers. SIFMA's mission is to promote policies and practices that work to expand and perfect markets, foster the development of new products and services and create efficiencies for member firms, while preserving and enhancing the public's trust and confidence in the markets and the industry. SIFMA works to represent its members' interests locally and globally. It has offices in New York, Washington D.C., and London and its associated firm, the Asia Securities Industry and Financial Market Association, is based in Hong Kong.

and how those uses could be modified to help minimize the unnecessary exposure of SSNs.

Securities firms use SSNs to facilitate confirmation of the identities of its customers. Because of their uniqueness, SSNs provide an effective means of identifying persons and confirming that the person who purports to be a customer is in fact the customer. This, in turn, helps securities firms detect and prevent identity theft or other fraud. The securities industry also uses SSNs as an integral part of programs designed to assure compliance with the Bank Secrecy Act and other laws and regulations that protect against permitting inappropriate transactions and require governmental filings. SSNs are also used by firms to identify multiple accounts of the same customer. Proper identification of accounts is particularly important in the securities industry in view of the fact that transactions often must be conducted promptly without delay because of rapidly changing market conditions. Securities firms recognize the sensitivity of SSNs and do not make them available to the general public, nor do they sell SSNs to other parties. Restrictions on their use by the securities industry and limits on the ability of securities firms to use SSNs to obtain information from governmental agencies could interfere with operational efficiency and interfere with the ability of the industry to prevent and detect criminal activity. Such limits could also have serious adverse effects on customers who have come to expect centralized service based upon the use of SSNs.

NATIONAL DATA SECURITY STANDARDS

The Task Force is considering whether to recommend that national data security requirements be established on all commercial entities that maintain sensitive consumer information. SIFMA believes that all companies that have custody of sensitive personal information have a responsibility to provide data security measures commensurate with the sensitivity and nature of the data and to protect sensitive personal information that consumers provide to them.

SIFMA also believes it is important for the Task Force to recognize that financial institutions are subject to section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act"), which requires financial institutions to implement appropriate administrative, technical, and physical safeguards designed to protect the security and integrity of customer information. This provision of the GLB Act underscores Congress's determination that financial institutions are obligated to protect customer information. The Securities and Exchange Commission (the "Commission") has adopted Regulation S–P, 17 C.F.R. Part 48, which requires all broker-dealers, investment companies, and investment advisers registered with the SEC to adopt written policies and procedures designed to institute administrative, technical, and physical safeguards for information pertaining to sensitive customer records and information. In addition, broker-dealers are subject to periodic examination by the SEC and Self-Regulatory Organizations for compliance with Regulation S-P. SIFMA believes that the Task Force's recommendations should take into account that the GLB Act already establishes a framework for extensive regulation of the securities industry and grants the Commission broad authority to require securities firms to implement and maintain appropriate safeguards. Therefore, any

recommendation should include a "safe harbor" for industries already subject to regulation in this area.

BREACH NOTIFICATION REQUIREMENTS

The Task Force is considering whether to recommend that a national breach notification requirement be adopted and requests comment on what should be the essential elements of such a requirement. SIFMA believes that a uniform national breach notification standard should be required.

SIFMA believes that a standard that links an obligation to notify consumers in the event of a breach with the crime of identity theft is appropriate. Any notification threshold should be tied to an actual threat to the consumer to which he or she might reasonably and effectively be expected to respond. We also believe that functional regulators like the Commission are best suited to monitor industry compliance. In this regard, SIFMA suggests that the Task Force consider the following recommendations:

Uniform National Standards

More than 30 states have enacted security breach legislation that requires disclosure of a breach of security of a computer system to the person whose sensitive personal information was compromised. Most state legislation does not provide an exception to coverage for entities that are functionally regulated at the federal level. Legislative requirements often vary from state to state. Such differences result in a patchwork of laws that are difficult to comply with and which often conflict. More importantly, the multitude of state and local laws is likely to result in confusion and potential harm to consumers. Consumers in different states could be subject to different security standards and levels of notification despite the fact that the harm they may suffer as a result of a security breach at the same institution is identical. For these reasons, SIFMA urges the Task Force to recommend legislation that results in a uniform national standard that pre-empts potentially conflicting state laws.

Harm Trigger

SIFMA believes that any national requirement for a notification in the event of a breach of security provide that consumers be notified when there is a significant risk that they will become victims of identity theft. Requiring notification if there is no significant risk of identity theft could have the unanticipated effect of overwhelming consumers with notices that might cause confusion and likely desensitize them to future notices. SIFMA believes that linking the notice requirement to a determination by the company, after reasonable investigation, that there is a significant risk that the consumer will become a victim of identity theft strikes the appropriate balance for both consumers and financial institutions alike.

Sensitive Personal Information

SIFMA believes that a notice to consumers should be required only in connection with a breach involving the kind of information that could be used to commit identity theft, such as unencrypted or unredacted sensitive personal information. This is the only type of information that most likely can be used to perpetrate identity theft. There is little reason to require notification be sent to consumers when the information obtained is of little or no practical value to an identity thief.

Functional Regulator Oversight and Rulemaking

Given the existing regulatory framework of the GLB Act and the expertise of functional regulators in addressing identity theft and data security, SIFMA believes that the Task Force should recognize the primary role of functional regulators in addressing these issues and support granting them exclusive rulemaking and oversight authority. Functional regulators examine institutions for compliance and possess authority to sanction those not in compliance. Accordingly, we recommend that the Task Force's recommendations addressing the security of data held by securities firms and other financial institutions subject to the GLB Act should provide that the functional regulators have the exclusive authority to develop and enforce regulations affecting institutions subject to their jurisdiction.

CONSUMER EDUCATION

The Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft through a national public awareness campaign. SIFMA believes that a campaign to inform consumers about the importance of protecting sensitive personal information and techniques they can use to prevent becoming victims of identity theft would be very useful. Such a campaign could advise consumers on such topics as proper disposal of computers that may contain personal information; how to prevent or detect spyware that intruders may have installed on their computers; how to avoid becoming a victim of phishing and pharming scams; and what steps to take if the consumer has become a victim of identity theft. SIFMA believes that based upon its extensive experience with issues relating to identity theft, the appropriate authority to co-ordinate a public education program should be the Federal Trade Commission.

VICTIM RECOVERY

The Task Force has issued an interim recommendation that Congress amend criminal restitution laws to allow identity theft victims to seek restitution from the identity thief for the value of their time in attempting to recover from the effects of the identity theft. SIFMA supports this recommendation in principle. However, we believe that it is important that any recommendation recognize that consumers should not be permitted to seek compensation for losses attributable to identity theft from a company whose systems have been breached and may itself be a victim of the crime.

TARGETED ENFORCEMENT INITIATIVES

The Task Force is considering whether to propose that law enforcement agencies undertake special enforcement initiatives focused primarily on identity theft. SIFMA supports encouraging law enforcement to prosecute the growing problem of identity theft. However, we believe that the securities industry would need to review the details of any such program before endorsing the specific elements.

The Task Force is also considering whether to recommend that federal agencies, including the SEC, the federal banking agencies, and the Department of Treasury review their supervisory and compliance programs to assess whether they adequately address identity theft and create sufficient deterrence. SIFMA believes that such a review can be useful and, accordingly, supports the Task Force's recommendation.

SIFMA appreciates the Task Force's consideration of our views on the important issue of identity theft. If we can provide additional information, please contact the undersigned at (202) 434-8400.

Sincerely,

Alan E. Sorcher
Vice President and
Associate General Counsel